

REMARKS/ARGUMENTS

Claims 1-28 remain in this application for consideration. Claims 14-19 and 21 have been currently amended to correct minor typographical errors. No new matter has been added.

I. Objection to the Abstract

The Abstract was objected to as containing an "implied phrase." Applicants have deleted the phrase "Described is" from the Abstract. Applicants believe that this amendment alleviates the concerns with the Abstract.

II. Rejection of claim 14-19 and 21-24 under 35 U.S.C. 112, second paragraph

Claims 14-19 and 21-24 were rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicants regard as the invention. Specifically, the Office Action indicates that the phrase "computer-implemented method" should be "computer readable medium". Regarding claim 21, the Office Action indicates that phrase "the second data structure" lacks insufficient antecedent basis. In accordance with the rejection, applicants have amended claims 14-19 to recite a "computer-readable medium" and claim 21 has been amended to recite the "configuration message." Applicants believe that the above overcomes the 35 U.S.C. 112, second paragraph rejection.

III. Rejection of claims 1-7 and 13-19 under 35 U.S.C. 102(e)

Claims 1-7 and 13-19 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,259,908 issued to Austin ("Austin"). Applicants respectfully disagree with the rejection. Austin fails to teach all the limitations of claims 1-7 and 13-19.

Claim 1 recites a computer-implemented method for maintaining configuration information on a mobile device. The method of claim 1 includes a step for "associating a security role with the received message." (Emphasis added). Claim 1 continues by reciting a step for "determining at least one configuration setting within the configuration information affected by the received message." (Emphasis added). Austin does not teach, at least, these limitations.

Austin teaches a method of limiting access, over-the-air, to data stored in a cellular telephone and limiting activation of a cellular telephone in a designated network. (Col. 12, lines 50-53). With reference to Figure 5 of Austin, Austin teaches that in step 504, the cellular telephone monitors whether configuration data of the cellular telephone has been requested by an entity. (Col. 10, lines 27-31). (Emphasis added). A base station that services the general area typically requests this configuration data. (Col. 10, lines 27-36). (Emphasis added). Austin does not teach anything more than monitoring to see if a request has been made.

Once a request has been made, the cellular phone sends a separate message back to the base station. (Col. 10, lines 42-45). The information in the message is used to calculate an authorization key at the base station. (Col. 11, line 60-col. 12, line 22). Austin continues by

teaching that the computer system of the base station has a program that decrypts the message that was sent by the cellular telephone. (Col. 11, lines 1-7). Once the computer decrypts the message, the computer at the base station generates an authorization key. (Col. 11, lines 7-11). The computer then transmits the key back to the cellular telephone. (Col. 12, lines 20-22). A key from the base station is then compared to a key in the cellular telephone. If the keys match, the cellular telephone is activated. (Col. 12, lines 27-33). Austin teaches the above because Austin pertains to the activation of a cellular telephone and as such, information needs to be exchanged between the cellular telephone and the base station. As is clear from Austin, Austin does not teach "receiving a message including a request associated with configuration information stored on the mobile device" and "associating a security role with the received message." Also, Austin clearly fails to teach "determining at least one configuration setting within the configuration information affected by the received message." Accordingly, Austin cannot possibly anticipate claim 1.

Regarding independent claim 13 of the present invention, claim 13 recites the step of "receiving a configuration message including an instruction associated with a configuration setting stored on the mobile device." Claim 13 also recites that step of "associating a security role with the instruction." Claim 13 further recites the step of "comparing the security role of the instruction with a security role associated with the configuration setting stored on the mobile device." For at least the same reasons set forth above in support of independent claim 1, applicants assert that claim 13 is allowable over Austin.

Regarding claims 2-7 and 14-19, Applicants assert that the limitations of those claims are not taught or otherwise suggested by the cited art. Moreover, claims 2-7 and 14-19 ultimately depend from independent claims 1 and 13, respectively. Claims 1 and 13 are clearly allowable as more fully set forth above. Therefore, claims 2-7 and 14-19 are also thought allowable for at least those same reasons.

IV. Rejection of claims 20 and 25-28 under 35 U.S.C. 102(e)

Claims 20 and 25-28 were rejected under 35 U.S.C. 102(e) as being anticipated by U.S. Patent No. 6,161,139 issued to Win et al. ("Win"). Applicants respectfully disagree with the rejection. Win does not teach all the limitations of the claims

Claim 20 is an independent claim that recites a "data structure associated with a configuration setting and a configuration service provider, the configuration setting being associated with a software component resident on the mobile device." Win does not teach or otherwise suggest such a limitation. Contrary to the citations in the Office Action, Table 1 of Win merely teaches a server configuration where several individuals have administrative powers on the network. As is best understood from Win, Table 1 is an illustrative table and does not represent fields in a data structure on a software component on a mobile device. (Column 16, lines 10-55). The column titled "FUNCTION" recites a list of various powers an employee might have when accessing a network. (Column 16, lines 10-55). Such powers might include viewing records, resetting a password or modifying records. (Column 16, lines 10-55). The four columns titled "ADMINISTRATION PRIVILEGE LEVEL" list four levels of administration, which indicate the "amount" of power a particular administrator might have when accessing a

network. (Column 16, lines 10-55). For example, one administrator might have the power to change passwords and another might not have this power. (Column 16, lines 10-55). Furthermore, column 26 of Win merely teaches a general overview of a computer system. Win simply does not teach a data structure associated with a configuration setting and a configuration service provider, the configuration setting being associated with a software component resident on the mobile device.

Claim 20 of the present invention also teaches that the data structure comprises "a first field including a security role associated with the configuration setting, the security role of the configuration setting identifying a setting privilege which must be had in order to access the configuration setting." Claim 20 continues by reciting that the data structure comprises "a second field including a security role associated with the configuration service provider, the security role of the configuration service provider identifying a provider privilege which must be had in order to make use of the configuration service provider." Again, the Office Action cites to Table 1 of Win as teaching this limitation. As stated above, Table 1 teaches the break down of computer access privileges in a company. Furthermore, as is best understood from the Win reference, Table 1 is merely an illustrative table of administrative functions and does not even remotely relate to a computer readable medium having a data structure with first and second field. Accordingly, applicants assert that Win does not anticipate claim 20.

Regarding claims 25-28, Applicants assert that the limitations of those claims are not taught or otherwise suggested by the cited art. Moreover, claims 25-28 ultimately depend from

independent claim 20. Claim 20 is clearly allowable as more fully set forth above. Therefore, claims 25-28 are also thought allowable for at least those same reasons.

IV. Rejection of claims 8-12 under 35 U.S.C. 103(a)

Claims 8-12 were rejected under 35 U.S.C.103(a) as being unpatentable over Austin, and further in view U.S. Patent No. 6,301,484 issued to Rogers et al. ("Rogers"). Applicants respectfully disagree with the Office Action. There is no suggestion in either of the references that they may be combined in the manner suggested. Furthermore, even if the above references could be combined for argument sake, they still fail to teach all the limitations of the claims.

Claim 8 recites "a stored setting having an assigned security role that identifies a privilege that an entity attempting to access the stored setting must satisfy in order to access the stored setting."

Claim 8 also recites that the "configuration message including an instruction that affects a configuration setting." Claim 8 further recites that "wherein if the configuration setting identified in the configuration message identifies the stored setting, and wherein if the source of the configuration message has sufficient privilege to access the stored setting, the configuration manager causes the instruction that affects the configuration setting to be processed." (Emphasis added). With regard to at least the above limitations, applicants rely on the explanation of the Austin reference set forth above in support for claim 1. Furthermore, the Rogers reference does not teach the limitations set forth in the Office Action. Accordingly, Claim 8 is clearly allowable under 35 U.S.C. 103(a).

Regarding claims 9-12 of the present invention, none of the cited art teaches or otherwise suggests the limitations of those claims. Furthermore, claims 9-12 ultimately depend from

independent claim 8. Claim 8 is clearly allowable as set forth above, and as such, applicants assert that claims 9-12 are also allowable.

IV. Rejection of claims 21-24 under 35 U.S.C. 103(a)

Claims 21-24 were rejected under 35 U.S.C. 103(a) as being unpatentable over Austin, and further in view of Win. Applicants respectfully disagree with the above-stated rejections. Applicants assert that the prior art cannot be modified in the manner suggested in the Office Action. Also, all the limitations of claims 21-24 are not taught or otherwise suggested by the cited art; the Austin and Win references have been misconstrued as set forth above. Furthermore, the Examiner's 35 U.S.C. 103(a) rejections depend from the above-stated 35 U.S.C. 102(e) rejection of claim 20. Claim 20 is clearly patentable under 35 U.S.C. 102(e), and therefore, the Office Action's 35 U.S.C. 103(a) assertions fail.

In view of the foregoing amendments and remarks, all pending claims are believed to be allowable and the application is in condition for allowance. Therefore, a Notice of Allowance is respectfully requested. Should the Examiner have any further issues regarding this application, the Examiner is requested to contact the undersigned attorney for the applicant at the telephone number provided below.

Respectfully submitted,

MERCHANT & GOULD P.C.



A handwritten signature of Ryan T. Grace.

Ryan T. Grace
Registration No. 52,956
Direct Dial: 206.342.6258

MERCHANT & GOULD P.C.
P. O. Box 2903
Minneapolis, Minnesota 55402-0903
206.342.6200